Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Inquiry Concerning 911 Access, Routing,	)	PS Docket 17-239
And Location in Enterprise	)	
Communications Systems	)	

Comments of
CISCO SYSTEMS, INC.

Executive Summary

The Enterprise Communications Systems ("ECS") market is diverse, complex, profoundly competitive, innovative, and supported by a highly developed ecosystem. One broad categorization of ECS might be to consider three types: 1) on premises hardware and software; 2) cloud solutions; and 3) over-the-top applications. There are permutations, variations, and combinations of these basic categories that exist ad infinitum. In the ecosystem, the role of manufacturers (vendors) is distinct from installers. It is distinct also from the enterprises that ultimately utilize the ECS through contracts with service providers. Specialized vendors offer "value add" solutions that work in concert with other ECS solutions. Moreover, enterprises will often install and rely upon multiple ECS solutions. They make their selections because a given ECS offers business value to their operations. They generally do not base procurement decisions on emergency call capability. As the Commission approaches the problem of how to improve ECS for emergency calling, this diversity and complexity is important to understand, including how that diversity relates to different technological capabilities among ECS platforms.

In this comment, Cisco urges the Commission to adopt a unified definition of ECS and to limit consideration in this particular docket to ECS that would be used for emergency calling. Specifically, this should be limited to include communications tools, whether IP-based or circuit-switched, that are intended and utilized by the enterprise to communicate on a point-to-point basis with phone numbers outside the enterprise other than a conference bridge. Simply put, there are ECS that are deployed and used in a way that would not be used for emergency calling. ECS for internal communications and conference bridges are two such examples.

Cisco also discusses some of the key issues that exist today, particularly with reference to dialing pattern, call back numbers, location accuracy, and routing. The dialing pattern issue has essentially been resolved by Congress, with two slightly different versions of Kari's law now passed in the House and Senate, awaiting conference. Once signed into law, this issue is clearly one that the Commission can take up and resolve. The inability to deliver a call back number that takes the Public-Safety Answering Point ("PSAP") back to the caller is an issue for some ECS. Location information, which is available for some ECS, presents some of the toughest challenges. Correct routing is a function of location.

Cisco suggests the largest gap by far is the problem of location information. For ECS, there is no single party that can resolve a caller's location in all cases. For example, a Virtual Private Network ("VPN") tunnel supporting a remote employee simply cannot ascertain where the employee is. However, employees – whether on premises or off – are often in range of and visible to a Wi-Fi access point, and the location of that access point can be used to deliver information about the caller's location – if and only if, standards existed to support it. In the VPN example, no provision exists in standards or technology to allow the softphone (or handset) to access and transmit the Wi-Fi access point location. Similar problems confront the use of Wi-Fi location for Web-based applications ECS, and when employees are "on the go." Cisco believes the Commission should convene a multistakeholder group to evaluate barriers to

providing location, and to recommend which barriers, if removed, would produce the greatest benefits.

In addition, Cisco recommends that the Commission consult with the PSAP community about offering a test facility that installers could use when configuring ECS for 911. Cisco is aware of well-intentioned installers who call a 911 center and announce they are making a test call. Despite the warning, such calls often result in the PSAP dispatching emergency services. Given the complexity of ECS, ensuring that upon configuration a call will get through is important, and this issue should be addressed.

Finally, Cisco reminds the Commission that the state commissions have been the primary regulators of ECS for decades, and are entities that the Commission should view as partners. In addition, some of the answers to the ECS questions posed in the Notice of Inquiry (NOI) are within the province of enterprises themselves. Not only are state commissions closer to these entities, but the Commission needs to find positive ways to incent enterprises to make good procurement and configuration decisions. Moreover, emergency services are typically provided by state, local, or municipal agencies.

Table of Contents

		Page
I.	Introduction and summary…..	1
II.	Future consideration of ECS and emergency calling needs to be targeted…..	5
III.	ECS market is diverse and complex…..	6
IV.	Key problems in supporting emergency calling for ECS…..	14
	A. Dialing pattern…..	14
	B. Call back number…..	15
	C. Location information delivery…..	16
	D. Routing to the nearest PSAP…..	17
V.	Gaps…..	18
	A. The untapped promise of Wi-Fi location…..	18
	B. No facility or protocol for test calls…..	21
	C. Additional considerations about ECS and emergency calling…..	21

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Inquiry Concerning 911 Access, Routing,	)	PS Docket 17-239
And Location in Enterprise	)	
Communications Systems	)	

Comments of
CISCO SYSTEMS, INC.

I. Introduction and summary

Cisco Systems, Inc. ("Cisco") is pleased to respond to the Commission's Notice of Inquiry in the above-captioned docket.[1] Cisco is a San Jose, California based company offering IP-based products, solutions and services to enterprise customers throughout the US and the world, both directly and through partner channels. In particular, Cisco offers a range of IP-based Enterprise Communications Systems ("ECS") that appear to fall within the scope of this inquiry.[2]

[1] Inquiry Concerning 911 Access, Routing, and Location in Enterprise Communications Systems, PS Docket 17-239, released September 26, 2017 (hereinafter "Notice" or "NOI").

[2] Cisco does not manufacture or sell traditional Private Branch Exchange products, and nothing in our comments should be construed to apply to that technology.

The ECS market is diversified and complex.[3] Different solutions are offered to different segments of the enterprise market based on size and mission of the enterprise. These solutions enable the enterprise to communicate internally as well as externally to partners, suppliers and customers, among others. The array of ECS solutions is formidable, including those based on traditional local exchange telephony (i.e., PBX), IP-based solutions in a wide spectrum of capacity and capability, various types of cloud offers, over-the-top applications, and combinations of these. While some solutions emphasize voice communications, increasingly voice is but one of the ways enterprises communicate – messaging, data and video are now as important in many cases. For those employees whose work is performed outside of a traditional office, being able to use a cell phone or softphone on a laptop to communicate with the enterprise is also key.

Based on Cisco's long-term engagement with enterprise customers, enterprises choose among these offerings based primarily on their ability to deliver a business benefit. Larger enterprises will often have multiple ECS solutions in use to meet a variety of specific—and sometimes mission critical—business functions. For example, ECS can help an enterprise be more productive, enable the enterprise to work more closely with its supply chain, service customers, and support remote workers. Some ECS solutions are externally imposed on an enterprise as a condition of doing business with a customer or vendor that already uses a

[3] On Oct. 23, 2017, Cisco announced its intent to acquire BroadSoft, a firm that also offers ECS products. As that acquisition will not close before NOI comments are due, nothing in this comment represents BroadSoft technology or capabilities or the views of the BroadSoft technology team.

particular communications pathway in its enterprise architecture. Some ECS solutions limit communications to a closed user group within an enterprise; others are designed to host conferencing capabilities; and others handle traffic that is closer to traditional point-to-point calls. Enterprises view the solutions that they utilize first from the vantage point that the solution is fit for purpose. Emergency calling is an appropriate goal for many ECS solutions. For some solutions, however, emergency calling simply does not make sense (e.g., a conferencing service), and for others it may be technically impossible (e.g., an internal ECS). In any event, emergency calling capabilities are very rarely a selection criteria for those making decisions about what ECS solutions address the specific business problem for which they are employed to address.

In fact, the number of times that ECS is used to reach emergency services is small compared to other modes of communication. The latest data available, reported by only a handful of states, showed that Multiline Telephone Systems ("MLTS") generated a fraction of emergency calls compared to other modes of communication.[4] This does not make the issue of improving emergency capabilities for ECS less compelling, but the statistic should inform the Commission as it considers any further steps in this docket. Cisco's recommendation is to prioritize solving problems concerning the location of emergency calls to Public Safety

[4] 2016 National 911 Progress Report, prepared by Booz, Allen and Hamilton under contract with the National Highway Transportation Safety Administration (NHTSA), December 2016 at 911.gov. For example, California reported less than 675,000 calls from ECS in 2015, compared to 26.7 million cellular calls received.

Answering Points ("PSAPs") based on the relative call volume from a particular segment of the technology market.

In addition, when ECS is utilized to summon emergency help, these systems must each in some way deliver communications to an emergency calling architecture that dates from the middle part of the 20th century. Although consolidation has occurred in some areas, PSAPs are typically organized around local jurisdictions, and are not laid out on a flat, networked IP architecture. Therefore, the communications must be delivered to the "right" PSAP – the one serving the jurisdiction of the caller, instead of a nationwide or even statewide PSAP system that can route the call. In addition, PSAP capabilities are at the early stages of evolving from voice only to text, data, and video . There currently is a lack of consistency among PSAPs with regard to their abiity to handle these various types of communications as the evolution depends on local funding. Some at the leading edge of Next Gen 911 can accept text, data, and or video—most cannot. Moreover, all the communication has to flow through the local exchange carrier network serving that PSAP, because that is how the PSAP connects to the public network. These are very real constraints on architectures and practices that if one were designing a greenfield system today would likely be discarded. The reality, however, is that we are unable to operate based on the assumption that these capabilities are universal—or even widespread. Therefore, enterprise emergency calling is an exercise in trying to conform modern technology to a system that in many ways is outdated. To be sure, Next Gen 911 will address some of these concerns, but not all.

This comment first seeks clarification on the scope of the ECS for the purposes of this docket, consistent with our understanding that ECS is the technological descendant of MLTS. Then, pursuant to the NOI questions, the comment describes the market and the ecosystem. The comment then reviews a few of the key problems in ECS that limit its utility in emergency calling, before turning to a few of the gaps that limit improvement. The comment concludes with some additional considerations, including thoughts on how the Commission might want to proceed, focusing first on implementing the future conferenced version of the two Kari's law bills that have now passed the House and Senate.

II. Future consideration of ECS and emergency calling needs to be targeted

The Notice of Inquiry casts a broad net, using the term "enterprise communications systems" in lieu of the former term "multi-line telephone systems" which the Notice asserts implies circuit switched technology. Because the Notice seeks to capture IP-based systems, the Commission decided to use the term "ECS." Except in reference to ECS being a IP version of MLTS, ECS is not defined in the text. At footnote 2, the Notice states that ECS "refer(s) to the full range of networked communications systems that serve enterprises, including circuit switched and IP-based enterprise systems." If that is intended as a scoping statement for a docket concerned with emergency calling, it is overly broad. Similarly, it would be useful for the Commission to explain why the more commonly used MLTS terminology was insufficient to meet its purposes and what is intended by the use of the newly adopted ECS terminology.

Cisco urges the Commission to clarify that the scope of this proceeding refers to those communications tools, whether IP-based or circuit-switched, that are intended and utilized by the enterprise to communicate on a point-to-point basis with phone numbers outside the enterprise other than a conference bridge. Where a technology is specifically deployed to support communication internal to the enterprise (i.e., it cannot support a call outside the enterprise), or where a tool is designed and used for conferencing services or other non-point-to-point communications, these should be designated as outside the scope of this proceeding. In at least these circumstances, there is no reasonable expectation on the employee's part that such internal or conferencing tools would be used to summon public emergency services.[5] By defining the scope of the proceeding to IP-based technologies that are intended and utilized by employees to communicate with phone numbers outside the enterprise other than a conference bridge, services that employees might utilize to summon emergency help will be appropriately captured for the purposes of an emergency services discussion.

Once there is a definition, then the Commision can begin parsing what is technically possible for a given offering, whether there are current barriers to emergency calling (such as the ability to convey location information), identify what those barriers are, determine what action or activity might address them, and assess the feasibility of those options and any attendant costs or benefits.

III. ECS market is diverse and complex

[5] The statutory definition of MLTS is of little help as it merely recites components of hardware and software that comprise MLTS. See 47 USC §1471.

The market for ECS serves a variety of business users and a variety of business purposes. From a vendor perspective, the market is robustly competitive, and consistent innovation is required to maintain market share. As a result, the array of products and solutions offered to enterprise users can be difficult to parse in a coherent fashion. For this reason, as will be detailed below, any future Commission actions in this docket must avoid rules that apply indiscriminately, without accounting for technical feasibility, service variations, and end user expectations.

At a very high level, one can sort through the chaos by defining services according to how they do what they do – on premises hardware and software, cloud solutions, and over-the-top applications. On-premises solutions are characterized by on-premises equipment and software that enables employees to dial out to the public network. For larger enterprises, such solutions will typically include a gateway to interface with a service provider. Cloud solutions, in contrast, host the operative call capability in the cloud, interacting with specific enterprise endpoints. The physical network by which a cloud-based call exits the enterprise to the public network varies. Over-the-top applications operate similar to interconnected VoIP services in the consumer environment – riding on top of a physical connection – and interconnecting with the public network at a service provider peering point. There are permutations, variations, and combinations of these basic categories that exist ad infinitum. For example, versions of VPN services (enabling a remote worker to tunnel to the enterprise network) exist for both on-premises and cloud-based offerings. Vendors offer a dizzying array of solutions as they attempt

to appeal to enterprises in various stages of network sophistication, with highly variable business environments, highly variable business sizes, and functional purposes.

Endpoints vary as well. Ethernet phones, Wi-Fi phones, softphones (such as phone capability available via software on a laptop or mobile device through an application), and of course the ubiquitous mobile phone are the typical devices that enterprises use.

Cloud-based ECS services also need to be understood based on the type of cloud that is being used. Cloud architectures are important because the cloud serves an important business requirement – to enable enterprises to be more agile in utilizing network capabilities. The use of cloud technologies allows for physical network resources, including networking functions, to be abstracted into a flexible, on-demand remote computing environment to enable easier and faster development and deployment of solutions, maintenance, and operations of enterprise networks. Clouds can be public – a cloud service provider offers an ECS solution hosted in the cloud to various enterprises. Clouds can be entirely private – maintained by a large enterprise for its own IT needs, including ECS. Hybrid clouds are a mix of on-premises technology deployments and cloud-based services. The presence of cloud-based services for emergency call capability is neither good nor bad – but it can have a differentiated impact on location capability, for example.[6]

[6] While use of cloud architectures is continuing to grow, it is important to recognize that cloud services are primarily used for corporate activities other than ECS. Moreover, most cloud "workloads" are consumer-based. About 25% of workloads are classified as business, a percentage that is roughly projected to remain the same through 2020. See generally Cisco's Global Cloud Index, https://www.cisco.com/c/en/us/solutions/service-provider/visual-

The ecosystem surrounding this diversity is unique to the enterprise market. There are vendors producing solutions, enterprises purchasing those solutions, installers (which could be the enterprise or a third party), service providers of various types, the employees, and of course the PSAPs and first responders. Understanding their roles and interrelationships is critical to assessing who might appropriate bear responsibilities related to emergency access. Core components of the ecosystem include the following:

First responders. These are police, firefighters, or ambulance crews summoned to a civic address based on a 911 call. It is worth briefly noting that for many enterprises, a civic address is simply a starting point. That address can represent a large building or facility containing many structures spread out over acres. To the extent a victim (or a colleague of a victim) can orally provide further direction to the dispatcher, then services can be provided in a more timely way. If not, the first responders may face a conundrum – locked gates, locked doors, and simply too much ground to cover to be effective. In fact, this problem of controlled or limited access to physical facilities where an emergency call may originate is not at all solved even if somehow all ECS solutions were able to convey precise caller location information. The fact is that there will likely always be a some issues requiring a level of coordination between the enterprise and first-responders.

---

networking-index-vni/index.html?POSITION=Cisco%2blink&COUNTRY_SITE=us&CAMPAIGN=GCI%2b2016&CREATIVE=go%2bURL%2bto%2bGCI%2bpage&REFERRING_SITE=Cisco%2blink#~stickynav=3

PSAPs. As noted above, the PSAPs themselves remain rooted in an emergency calling systems that pre-date IP-based services. This is no fault of theirs, as the PSAP community has diligently worked toward defining next generation services, labored for decades under unfair funding conditions, and, in some cases, has faced challenges in working with local carriers. A growing contingent of PSAPS have migrated to next generation 911, and are now capable of accepting IP-based communications, although this is far from universal. But it remains the case that a call seeking emergency help must find its way to the local PSAP through a serving local exchange carrier, and subject to a tightly defined set of data constraints that enable the PSAP to process the call data. Regardless of the level of sophistication of the PSAP, two pieces of data remain critical to the emergency response community – location and a call back number.

Vendors. At the other end of the ecosystem are ECS vendors. These are manufacturers of hardware and software, vendors offering cloud services, or applications developers that produce ECS enabling enterprises to reach phone numbers outside of the enterprise, on the public network. Depending upon the solution architecture or design, vendors can design systems capable of supporting 911 and prefix-911 dialing patterns, call back numbers in many cases (but not all), and where technically possible, location data. Vendors also offer complementary solutions. In the emergency services case, there are vendors such as West Corporation that produce solutions to complement or augment a solution offered by another vendor, such as Cisco.[7]

[7] https://www.west.com/?s=emergency+calling&lang=en

Enterprises. Enterprises purchase ECS, and often multiple different ECS, from a single vendor or multiple vendors. Often the ultimate purchase is made via a contract with a vendor's partner or value-added reseller in its distribution chain. In the vast majority of cases, it is the enterprise that contracts with the public network provider to carry its traffic to and from the public network. For enterprises that need access to the local exchange for business purposes, local exchange services are mandated by states to include emergency calling. However, use of the local exchange is not universally applicable to all forms of ECS. Some ECS offerings are architected to utilize a centralized service provider, and that centralized service provider may or may not include emergency call capabilities in their offering.[8] If not, enterprises will need to engage a local exchange services provider separately or possibly a national emergency call services provider that can initially receive a 911 call and direct it to the correct PSAP.

In addition to the purchasing decision and contracting with a service provider, the enterprise directs its installer in the configuration of the system. Configuration "guides" produced by vendors are just that – guides. Upon installation, the ECS must be configured to work within a specific enterprise environment and with the requirements that the enterprise has deemed necessary or desirable. Configuration requires a number of decisions to be made, company-specific data to be entered into the system, and connection to the public network to

[8] There are cases where the centralized service provider is bundled with the ECS, although the more common approach is to have the customer contract separately with the centralized service provider.

be made. One other role of the enterprise is important. If emergency call capability is not provided on a given ECS, the enterprise should warn employees not to attempt to use it to reach emergency services and to use another ECS instead. This can be accomplished through training or warnings within the system itself.

Installers. Installers must configure a solution by making configuration selections across a variety of parameters – not limited to, but including, emergency call capability. This includes establishing the dialing pattern for emergency calls, how calls will route to the public network, and where it will interface with the public network (which could be a different jurisdiction). It also involves obtaining phone numbers to support the ECS, configuring the system (if possible) to support emergency call back, and enabling location (if possible). In doing so, the installer is following the enterprise's specific direction. Once complete, configuration brings the call capability of the system to life specific to, and within, that enterprise's network. Most significantly for the Commission's purposes, vendors are typically not in the installation business. Configuring ECS is an entirely different line of business than manufacturing ECS. Procurement of numbers and interconnection to the public network are two examples of why configuration is not a function associated with manufacturing, but a function of installation.[9]

[9] For example, the two versions of Kari's Law that that have passed the House and the Senate recognize this distinction between vendors and installers with respect to configuring emergency dialing patterns. Kari's Law Act of 2017, S.123, Report 115-124 (1st Session 115th Congress), adopted Aug. 3, 2017 by unanimous consent, Congressional Record at S4818-S4819; Kari's Law Act of 2017, HR 582 (1st Session 115th Congress) adopted Jan. 23, 2017 by unanimous consent at Congressional Record H588. The text of HR 582 has also been incorporated into a pending House FCC Reauthorization Bill, H.R._, a bill to amend the Communications Act of 1934 to reauthorize appropriations for the Federal Communications Commission.

Even small business solutions, where configuration tools can be provided on the web, require the user to configure its system and then separately contract with a service provider to obtain the requisite number of phone numbers.

Service providers. Service providers are active in the ECS ecosystem in any number of ways. They may be offering ECS to a business customer, as the traditional service providers do as part of local exchange service. They may contract with the enterprise to carry its traffic to and from a gateway or peering point – the service providers may be local telephone service providers, backhaul providers or centralized IP-based services providers. Some centralized providers may offer national 911 capability, which is helpful when enterprise calls that lack reliable location data need to be forwarded to the correct PSAP.[10]

Employees.[11] Those who are summoning emergency help may or may not be able to utilize ECS to make an emergency call. Indeed, as the 2016 NHTSA report indicates,[12] when it comes to emergency calling, mobile phones reign supreme. There is no logical reason to believe employees react any differently while on their employer's premises than they would outside of a work premises. Of course, given the wide variety of ECS available, it is entirely possible that an enterprise may have enabled its employee's mobile phones to be equipped

[10] Traditional local exchange or wireless service providers also contract with 911 service providers to meet state or federal 911 requirements.

[11] This category includes both guests and customers who are on the enterprise premise.

[12] See footnote 4, supra.

with ECS capability, such as the capacity to initiate a VPN and/or to open an ECS application for example. Therefore, ECS on an employee's mobile phone might be used. If the employee does not have an ECS-equipped mobile telephone, or the employee in the emergency does not choose to rely on that capability (e.g., the application might not be open when the emergency occurs) then using ECS to summon help depends upon chance – the employee being at or near an ECS endpoint capable of dialing when an emergency occurs. When ECS is used to summon emergency help, it is probably associated with the presence of a dialing pad that easily and quickly allows someone to dial the emergency digits in the midst of a confusing, dangerous and/or possibly painful set of circumstances. If that's true, then a desk phone endpoint, or possibly a softphone if a dialing pad is open on the screen, are in all likelihood what employees use. Unfortunately, there is no public data to inform the Commission of what actually happens, but this would logically explain the remarkably low percentage use of ECS to reach emergency services.

IV. Key problems in supporting emergency calling for ECS

A. Dialing pattern

The issue of the digits that are used when ECS is invoked to summon emergency help has effectively been decided by the Congress.[13] Both the House and Senate have passed a version of Kari's law, and while the versions are somewhat different, the operative

[13] In the House, the original bill passed in the last Congress and identical language has now been recommended out of the Communications and Technology Subcommittee as part of the FCC Reauthorization Act of 2017. See HR 4167 (114th Congress); Senate Bill 123 (115th Congress).

requirements are identical. Under the bills as passed, enterprises must enable MLTS to initiate a 911 call with no prefix to reach emergency help. Enterprises may also enable 9-911 if they wish, but they must enable 911. Most importantly, both bills recognize that the dialing pattern issue is made as part of configuration conducted by the installer when the installer is setting up the interface to the public network. Cisco recommends that the installer configure the system with both dialing patterns so that caller will reach emergency services regardless of the dialing pattern used. However, some enterprises have not insisted that the configuration support both dialing patterns. One concern has been 911 mis-dials stemming from an employee placing toll calls – e.g., dialing 9+1+10 digits. There are alternative solutions to this mis-dial issue, however, such as a brief local ringback before the call is delivered to the PSAP to make sure the employee is aware that he or she is summoning emergency help. Further Commission action in this docket should look to implement these bills once they are conferenced and signed into law. Among the issues the Commission will have to consider – the scope of MLTS to which the law applies; where the 911 dialing pattern is available in an existing MLTS deployment but not configured, how to encourage compliance with the new law; how to enable testing, and the role of the state regulatory authorities with either oversight authority over the operations of the particular organization or of emergency call routing generally.

B. Call back number

Depending upon the ECS and its configuration, provision of a call back number may be reasonably achievable or may be difficult. Many offerings have a specific phone number assigned to an end device. Even in the case of extension phones, it may be possible to assign

those phones a virtual number that would permit call back. On other hand, there are ECS examples where a call back from the PSAP would reach only the enterprise's main number. In addition, the call back number could have location significance – the caller may not be at the enterprise's main location. One technology differentiator here is whether the solution offers static phone number assignments or dynamic ones, and whether the location delivery function is separate from the call back number.

C. Location information delivery

For some ECS, location based on civic address is available. For others, provision of an accurate civic address is impossible. For example, a large enterprise with a complete on-premises ECS that includes a location solution (such as Cisco Emergency Responder) will deliver civic address information associated with a 911 call placed on that system. If the location capability is static, however, and requires manual update of phone location, the system is less likely to deliver accurate information. To the extent location capability can be updated automatically whenever a device is plugged in to the network, then the more accurate it will be. In such a case, additional location information can be delivered that provides a more precise location within the enterprise than the civic address of the enterprise front door.

In contrast, accurate location data cannot be generated from a VPN connection that, to the enterprise, appears as an IP address corresponding to the enterprise end of the IP tunnel. Callers could be thousands of miles away from the enterprise. While generating accurate location for a VPN caller is not possible based on current technology or standards, it might be possible for the calling endpoint to detect its location based on local infrastructure (e.g., Wi-Fi

access point) and to transmit this information over a VPN. But as described below, this type of solution remains undeveloped as it requires a multi-stakeholder approach to the problem.

Over the top solutions, relying on applications for business communications face the same challenges that consumer over the top interconnected VoIP services do. Employees can be prompted to enter updated location information. As with the VPN example, Wi-Fi location data might be available to mitigate this gap, but solutions remain undeveloped.

Finally, cloud-based deployments can complicate location. Many location techniques in ECS pre-date cloud, and work best with on-premises network deployments.

D. Routing to the nearest PSAP

This issue is a function of configuration and the decisions enterprises make when interconnecting to the public network with a service provider. Moreover, it is entirely dependent on the availability of accurate location data. As a result, some ECS deployments support highly accurate routing of an emergency call to the nearest PSAP, while others do not. Even when location data is available, sometimes a distant PSAP can receive a call. For example, it is the enterprise that decides how its outbound traffic flows to the public network. Small or satellite offices are often configured so that all traffic first flows via a private connection to a larger office, where calls destined for the public network are handed off to a service provider at the gateway device. Enterprises should arrange with the service provider to backhaul calls that are local to the satellite office to that satellite office's exchange area for completion, but

sometimes enterprises do not choose to do that. If so, then the wrong PSAP answers the emergency call.

Some service providers maintain national 911 call centers where calls without accurate location data (e.g., extension phones) might be routed first for hand off to the nearest PSAP. Of course, this solution works when the caller can speak and identify their actual location.

V. Gaps

A. The untapped promise of Wi-Fi location

Wi-Fi is the technology with the most promise for improving location capability for ECS. First, Wi-Fi is the most ubiquitous technology, present throughout the enterprise, powering connectivity for remote workers, and connectivity "on the go." Second, even for a Wi-Fi network not optimized to deliver location, a Wi-Fi system can deliver location within roughly 20 meters of accuracy. Optimized for location, the data is much better – a few meters. And home routers are associated with a civic address. An endpoint that can see a Wi-Fi router and learn its location would be a boon for a number of ECS offerings that are today location challenged. But no industry standards exist to leverage that Wi-Fi location and utilize it for ECS emergency calling.[14]

The biggest problems in deriving location could potentially be solved to a significant extent if Wi-Fi location could be utilized more broadly – on premises and off. For example,

[14] The NEAD discussed below addresses service provider Wi-Fi for enhancing location of mobile network calls.

endpoints within an enterprise tend to be nomadic, sometimes significantly so as companies have moved to embrace open office designs where employees have no fixed work location. Static mapping solutions that assign an employee, a phone number and a fixed work location typically no longer are relevant, unless the enterprise takes active measures to prohibit the relocation of an IP phone, which is rare. And for softphones, assigning a static location is not possible – the softphone might be on premises or off premises at any given point in time. Moreover, a Wi-Fi source of data location could both improve location for on-premises ECS and for cloud-based ECS.

Alternatively, Wi-Fi location could help address other gaps associated with technologies such as VoIP. Over the top ECS, or VoIP-enabled applications, are subject to the same laws of physics as interconnected over the top VoIP services to consumers. The application does not access location available natively on the mobile device. As a result, these types of ECS typically are generally associated with warnings to employees not to use them for emergency calling, or like their consumer counterparts, provide an encouragement for the employee to register their actual location should an emergency call be necessary. As with consumer versions of this technology, the likelihood of a better solution appears to be quite low. A different location data source will likely be needed, such as the location information that can be derived from Wi-Fi. This issue affects location data delivery but also routing of calls to the nearest PSAP.

The use of Wi-Fi as a location source has been partially reflected in the Commission's drive to improve location accuracy for mobile phones. As Cisco understands it, the National

Emergency Address Database ("NEAD") will collect registration data of service provider Wi-Fi access points so that mobile phone location can be cross referenced against the registered location of a Wi-Fi access points. This mechanism no doubt holds appeal for service providers who can mutually benefit from the NEAD, and one might expect that a number of Wi-Fi location points will be added to the NEAD. But the system does not address enterprise Wi-Fi networks or how service provider Wi-Fi can be leveraged to deliver location information to emergency ECS calls.

When the Commission was considering mobile phone location improvements, Cisco did propose a mechanism whereby enterprises might be positively incented to receive queries from e911 service providers to determine if an enterprise Wi-Fi network could see the calling phone and thereby triangulate location.[15] In the final order, however, the Commission did not choose to list this among the improvements it wanted to see in the mobile location system, and to Cisco's knowledge, work on this idea has not progressed. In Cisco's view, this was a missed opportunity to bring enterprises in to 911 ecosystem in a positive way, particularly since many calls from enterprise to emergency services are likely to be from mobile phones. Cisco would recommend that the Commission revisit this concept in the furture as possible solution or at least adjunct source of useful data to improve the accuracy of location information for emergency callers.

[15] See, e.g., Ex Parte in Amending the Definition of Interconnected VoIP Service in Section 9.3 of the Commission's Rules, GN Docket No. 11-117; Wireless E911 Location Accuracy Requirements, PS Docket No. 07-114; E911 Requirements for IP-Enabled Service Providers, WC Docket No. 05-196, filed by Cisco Systems and TCS, October 16, 2014 at https://ecfsapi.fcc.gov/file/60000973868.pdf.

B. No facility or protocol for test calls

Given the diversity and complexity of ECS, a significant gap remains in testing. No installer would configure ECS and then fail to place a test call to a public network to ensure the system is working properly. Yet, no facility or protocol exists to allow that same installer to make sure that the emergency call configuration can work. Cisco is aware in some cases of conscientious installers dialing 911 and announcing that they are making a "test call" – an announcement which is of course ignored by the call dispatchers, who then proceed to dispatch emergency services anyway. The Commission should ask the PSAP community to work toward a solution so that a test environment can be created. This is very important in light of the complexity and diversity of ECS.

C. Additional considerations about ECS and emergency calling

First, the role of state regulation is an important one for the Commission to consider with respect to ECS. This is the one VoIP example where states have occupied the regulatory field (although arguably not in a consistent or holistic fashion). It is also an example where the facts – an employee summoning emergency help from the local PSAP – do not on their face have interstate overtones to it, at least for most ECS emergency calls. And finally, it is an example where enterprises themselves to some degree hold the key to improvements. Improvements are going to require new technology solutions, which means that enterprises will need to decide to procure and/or install them. And, as discussed above, enterprises make numerous configuration decisions that can positively, or negatively, impact emergency calls. Incentivizing more robust emergency calling capability is likely going to be more important

than, for example, attempting to enforce a federal rule against enterprises nationwide. State commissions, who are closer to enterprises, and the emergency responders who are local to those enterprises could be strong allies. On the other hand, where Congress has acted to provide explicit direction to the Commission, as will likely be in the case with Kari's law, the Commission is free within the bounds of the federal statute to implement what Congress has directed.

Second, to the extent the Commission considers new requirements on ECS that are technically feasible, industry will need time to develop these and implement them. The versions of Kari's law passed by the House and Senate are an example of that principle in practice, giving industry time to implement the dialing pattern requirements of these bills.

Third, given the complexities and what can only be described as a very short list of improvements that are arguably "low hanging fruit," the Commission might first want to determine in consultation with industry and the PSAP community what aspects of ECS improvements offer the biggest measure of return to the PSAPs and focus on those. As noted above, when doing so, we recommend keeping in mind the relatively small number of calls that come to PSAPs from ECSs as compared to other sources of calls. ECS can be improved and issues should be addressed. However, the Commission should also proceed in a risk-based manner and prioritize the greatest sources of call where location is not readily ascertainable.

The dialing pattern issue is essentially one handed to the Commission by Congress and should be taken up, but the Commission should give some thought to how it will deploy scarce

resources to address other improvements in emergency calling for ECS and whether those solutions are facilitated by best practices, regulation, or encouragement of multi-stakeholder processes. Utilization of the Technical Advisory Committee is another option here. Regardless of what process might be convened, in Cisco's view the key issue is determining what obstacles stand in the way of delivering improved location information on different ECS platforms, including analyzing the extent to which multistakeholder actions are required.

Cisco looks forward to reviewing the record filed in response to this NOI, and in working with the Commission on ECS and emergency calling.

Respectfully submitted,

Cisco Systems, Inc.

By: Mary L. Brown
Senior Director, Spectrum and Technology Policy
601 Pennsylvania Ave. NW 9th floor North
Washington DC 20004
(202) 354-2923

November 15, 2017